(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号

特許第6095289号
(P6095289)

(45)発行日　平成29年3月15日(2017.3.15)　(24)登録日　平成29年2月24日(2017.2.24)

(51)Int.Cl.		F I		
G06F 1/30	(2006.01)	G06F	1/30	X
G06F 1/32	(2006.01)	G06F	1/32	Z
G06F 11/14	(2006.01)	G06F	11/14	641D

請求項の数 7　(全 10 頁)

(21)出願番号　特願2012-164610(P2012-164610)
(22)出願日　平成24年7月25日(2012.7.25)
(65)公開番号　特開2014-26374(P2014-26374A)
(43)公開日　平成26年2月6日(2014.2.6)
審査請求日　平成27年7月22日(2015.7.22)

(73)特許権者　000001007
キヤノン株式会社
東京都大田区下丸子３丁目３０番２号
(74)代理人　100145827
弁理士　水垣　親房
(74)代理人　100199820
弁理士　西脇　博志
(72)発明者　秋庭　朋宏
東京都大田区下丸子３丁目３０番２号　キヤノン株式会社内

審査官　田川　泰宏

最終頁に続く

(54)【発明の名称】情報処理装置、情報処理装置の制御方法、及びプログラム

(57)【特許請求の範囲】
【請求項１】
情報処理装置であって、
前記情報処理装置の第１の電力状態から前記情報処理装置の少なくとも一部に電力が供給されない第２の電力状態へ遷移する前に、前記情報処理装置が実行するアプリケーションの状態を示す情報を記憶する揮発性記憶手段と、
前記揮発性記憶手段に記憶される前記アプリケーションの状態を示す情報を、前記情報処理装置が前記第２の電力状態である間保持する不揮発性記憶手段と、
前記情報処理装置が前記第１の電力状態から前記第２の電力状態に移行する場合に、前記アプリケーションの状態を示す情報のうちの前記揮発性記憶手段の特定領域以外に記憶される情報を前記不揮発性記憶手段に暗号化せずに記憶し、続いて、前記アプリケーションの状態を示す情報のうちの前記揮発性記憶手段の前記特定領域に記憶される情報を暗号化して前記不揮発性記憶手段に記憶する制御を行う制御手段と、
を備えることを特徴とする情報処理装置。
【請求項２】
前記制御手段は、前記情報処理装置が前記第２の電力状態から前記第１の電力状態に移行する場合に、前記不揮発性記憶手段に暗号化された記憶された情報を復号化して前記特定領域に記憶し、続いて、前記不揮発性記憶手段に暗号化されずに記憶された情報を前記特定領域以外の領域に記憶する、ことを特徴とする請求項１記載の情報処理装置。
【請求項３】

前記不揮発性記憶手段は、ハードディスクであることを特徴とする請求項１記載の情報処理装置。
【請求項４】
前記不揮発性記憶手段は、電池を用いて情報を保持する半導体メモリであることを特徴とする請求項１記載の情報処理装置。
【請求項５】
前記半導体メモリは、前記情報処理装置に対して着脱可能なコントローラボードに設けることを特徴とする請求項４記載の情報処理装置。
【請求項６】
揮発性記憶手段と不揮発性記憶手段とを有する情報処理装置の制御方法であって、
前記情報処理装置の第１の電力状態から前記情報処理装置の少なくとも一部に電力が供給されない第２の電力状態へ遷移する前に、前記情報処理装置が実行するアプリケーションの状態を示す情報を前記揮発性記憶手段に記憶する揮発性記憶工程と、
前記揮発性記憶手段に記憶される前記アプリケーションの状態を示す情報を、前記情報処理装置が前記第２の電力状態である間前記不揮発性記憶手段に保持する不揮発性記憶工程と、
前記情報処理装置が前記第１の電力状態から前記第２の電力状態に移行する場合に、前記アプリケーションの状態を示す情報のうちの前記揮発性記憶手段の特定領域以外に記憶される情報を前記不揮発性記憶手段に暗号化せずに記憶し、続いて、前記アプリケーションの状態を示す情報のうちの前記揮発性記憶手段の前記特定領域に記憶される情報を暗号化して前記不揮発性記憶手段に記憶する制御を行う制御工程と、
を備えることを特徴とする情報処理装置の制御方法。
【請求項７】
請求項６記載の情報処理装置の制御方法をコンピュータに実行させることを特徴とするプログラム。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、アプリケーションを実行してデータ処理を行う情報処理装置、情報処理装置の制御方法、及びプログラムに関するものである。
【背景技術】
【０００２】
データ処理装置のシステムを構成するソフトウエア規模の肥大化に伴い、電源スイッチ操作からシステムの起動が完了するまでの時間（システム起動時間）は増大する傾向にある。このような起動時間増大に対する解決策の一つとして、ハイバネーション技術が活用されている。
【０００３】
ハイバネーションとは、任意の時点におけるシステムの揮発性記憶装置（メモリ）上の情報をＨＤＤ（ＨａｒｄＤｉｓｋＤｒｉｖｅ）やＳＳＤ（ＳｏｌｉｄＳｔａｔｅＤｒｉｖｅ）やＵＳＢ（ＵｎｉｖｅｒｓａｌＳｅｒｉａｌＢｕｓ）メモリ等の不揮発性記憶装置に退避保存しておき、次回システム起動の際に、退避保存しておいた情報を揮発性記憶装置に書き戻すことによって、システムの状態を「退避保存時の状態」に復元する技術のことである。
【０００４】
上記システムの状態を「退避保存時の状態」に用いられるメモリ上の情報には、パスワードなどの機密情報が含まれている可能性がある。ここで、ハイバネーションを使用しないのであれば、それらの情報は装置の電源を落とすことで消失されるため、第三者が取得することは非常に困難である。
【０００５】
しかしながら、ハイバネーションを使用する場合は、その情報が不揮発性記憶装置に記

憶されるため、ＨＤＤ等の着脱可能な不揮発性記憶装置であった場合、機密情報が第三者に取得される可能性が高くなる。

【０００６】

このような対策として、特許文献１では、データ処理装置内のシステムオンチップ（ＳｏＣ）の内部にデータ暗号化・復号化の処理部分を有し、外部からハイバネーション信号の入力があった場合には、その間のメモリアクセスを暗号化・復号化することで、機密情報を保護している。

また、ＬＵＫＳ（Ｌｉｎｕｘ(登録商標) Ｕｎｉｆｉｅｄ Ｋｅｙ Ｓｅｔｕｐ）等のように、不揮発性記憶装置上のファイルシステムを暗号化ファイルシステムにすることで、不揮発性記憶装置に保存する際にソフトウエアでメモリ上の情報全体を暗号化する方法もある。

【先行技術文献】

【特許文献】

【０００７】

【特許文献１】特開２００８－２０４４５９号公報

【発明の概要】

【発明が解決しようとする課題】

【０００８】

上記ＳｏＣなどのハードウェアで暗号化する場合、その機構を情報処理装置のＳｏＣの内部に追加する必要があるため、安価に実現することができない。

【０００９】

また、ＬＵＫＳのようにソフトウエアで暗号化する場合、データ処理装置が備えるメモリ全体に対して処理を行うことになるので、暗号化・復号化の処理時間の分、情報処理装置において要求される起動時間の短縮への寄与が少なくなってしまう。

【００１０】

一方で、暗号化の対象となるメモリに注目すると、汎用の情報処理装置（ＰＣ）などでは、様々なアプリケーションが動作しメモリ上にデータを残すため、暗号化が不要な領域を特定することができない。結果として、情報処理装置が備える全メモリを暗号化の対象とせざるを得ないため、暗号化処理時間の短縮が計れない。

また、情報処理装置の全メモリを対象としてしまうため、適切な暗号化のアルゴリズムを使用しないと、暗号化後のデータのパターンから暗号アルゴリズムが特定されてしまう等の課題があった。

【００１１】

本発明は、上記の課題を解決するためになされたもので、本発明の目的は、情報処理装置が通常電力状態から省電力状態に移行する要因があった場合に、情報処理装置の状態を示す情報のうちの揮発性記憶手段の特定領域に記憶される情報については機密性を保持した状態で不揮発性記憶手段に対して短時間に退避できる仕組みを提供することである。

【課題を解決するための手段】

【００１２】

上記目的を達成する本発明の情報処理装置は以下に示す構成を備える。

情報処理装置であって、前記情報処理装置の第１の電力状態から前記情報処理装置の少なくとも一部に電力が供給されない第２の電力状態へ遷移する前に、前記情報処理装置が実行するアプリケーションの状態を示す情報を記憶する揮発性記憶手段と、前記揮発性記憶手段に記憶される前記アプリケーションの状態を示す情報を、前記情報処理装置が前記第２の電力状態である間保持する不揮発性記憶手段と、前記情報処理装置が前記第１の電力状態から前記第２の電力状態に移行する場合に、前記アプリケーションの状態を示す情報のうちの前記揮発性記憶手段の特定領域以外に記憶される情報を前記不揮発性記憶手段に暗号化せずに記憶し、続いて、前記アプリケーションの状態を示す情報のうちの前記揮発性記憶手段の前記特定領域に記憶される情報を暗号化して前記不揮発性記憶手段に記憶する制御を行う制御手段と、を備えることを特徴とする。

【発明の効果】
【００１３】
本発明によれば、情報処理装置が通常電力状態から省電力状態に移行する要因があった場合に、情報処理装置の状態を示す情報のうちの揮発性記憶手段の特定領域に記憶される情報については機密性を保持した状態で不揮発性記憶手段に対して短時間に退避できる。
【図面の簡単な説明】
【００１４】
【図１】情報処理装置のハードウエア構成を示すブロック図である。
【図２】図１に示したＲＡＭの論理的構造を示す模式図である。
【図３】情報処理装置の電力制御方法を説明するフローチャートである。
【図４】情報処理装置の電力制御方法を説明するフローチャートである。
【図５】情報処理装置の電力制御方法を説明するフローチャートである。
【図６】情報処理装置の電力制御方法を説明するフローチャートである。
【発明を実施するための形態】
【００１５】
次に本発明を実施するための最良の形態について図面を参照して説明する。
＜システム構成の説明＞
〔第１実施形態〕
【００１６】
図１は、本実施形態を示す情報処理装置のハードウエア構成を示すブロック図である。本例は、所定のデータ処理要求を受け付けない状態に遷移した場合、省電力状態に遷移させる前に、揮発性記憶手段に記憶された情報を不揮発性記憶手段に退避させる制御を行う情報処理装置である。情報処理装置としては、ハイバネーションモードを備える装置であれば、データ処理の機能の別には本発明の適用は妨げられない。したがって、当該情報処理装置には、データ処理を行うパーソナルコンピュータや、データ送受信装置、プリンタ装置、スキャナ装置、プリント機能、スキャナ機能、データ通信機能を備える複合装置等が含まれる。
本実施形態では、不揮発性記憶装置としてＨＤＤを用いた例を記載するが、他の不揮発性記憶装置（例えば、ＳＳＤ、ＵＳＢメモリ）を用いても構わない。
【００１７】
図１において、１００は情報処理装置で、ハードディスク（ＨＤＤ）１０２に記憶されたソフトウエアを実行するＣＰＵ１０１を備え、ＣＰＵ１０１はシステムバス１１３に接続される各デバイスを統括的に制御する。なお、ＣＰＵ１０１は、アプリケーションが使用する特定情報を揮発性記憶手段（本実施形態では、ＲＡＭ１０３）の特定領域（後述する暗号化対象領域２０２）に保持させながら、データ処理を行う。
【００１８】
ＨＤＤ１０２は、ソフトウエアやデータ等を保持し、電源供給が絶たれてもその内容を保持する不揮発性の記憶装置である。１０３はＲＡＭで、ＣＰＵ１０１のメインメモリ、ワークエリア等として機能する。１０４は割り込み制御部（ＩＮＴＣ）で、電源スイッチ（ＰＯＷ－ＳＷ）１０５と接続されている。ＰＯＷ－ＳＷ１０５がＯＦＦされると、ＩＮＴＣ１０４に伝達され、ＣＰＵ１０１は電源ＯＦＦを検知できる。また、ＰＯＷ－ＳＷ１０５は、電源ユニット１０７とも接続されており、電源ＯＮされると装置全体に対して電源が供給される。ＳＲＡＭ１０６は電池１０６Ａによりデータが保持される記憶装置で、通常はコントローラボード上配置される。また、本実施形態においては、当該コントローラボードは、情報処理装置から着脱可能にバス接続されている。１０８はネットワークコントローラ（ＮＩＣ）で、ネットワーク１０９を介して他の情報処理装置と通信可能に接続されている。電源ユニット１０７は、ＣＰＵ１０１からの指示あるいは、ＮＩＣ１０８から所定時間、データ受信処理が実行されない場合に、データ処理の復帰に必要なデバイスを除いて、電源の供給が不要なデバイスへは電源を供給しない省電力モード制御を行う。また、電源ユニット１０７は、省電力モード制御により低電力状態で、ＮＩＣ１０８が

データを受信したり、電源スイッチ（ＰＯＷ－ＳＷ）１０５がＯＮにする指示を検知した場合、各デバイスに必要な電源の供給を再開したりする電力制御を実行する。

【００１９】

この際、ＣＰＵ１０１は、電源スイッチ（ＰＯＷ－ＳＷ）１０５により電源をオフ状態（遮断状態）へ遷移させる指示を受け付けた場合、電源ユニット１０７がＣＰＵ１０１の電源の供給を停止する前に、ＣＰＵ１０１は、実行していたアプリケーションの状態を正常に復帰させるために必要なＲＡＭ１０３の情報をＨＤＤ１０２に退避させる。また、電源スイッチ（ＰＯＷ－ＳＷ）１０５により電源をオン状態へ遷移させる指示を受け付けた場合、電源ユニット１０７がＣＰＵ１０１への電源の供給を再開した際に、ＣＰＵ１０１は、ＨＤＤ１０２に退避させた情報をＲＡＭ１０３に復帰させる制御を実行する。

なお、本実施形態では、アプリケーションの起動に際して、パスワード等の機密情報を入力する必要がある場合、当該機密情報を特定の情報として、かつ、ＲＡＭ１０３上の特定の領域（暗号化対象領域２０２）で管理している。なお、複数のアプリケーションが起動している場合には、アプリケーションに対応づけられた特定の情報が複数記憶されている場合がある。

【００２０】

また、ＣＰＵ１０１は、電源スイッチ（ＰＯＷ－ＳＷ）１０５により電源をオフ状態へ遷移させる指示を受け付けた場合、ＲＡＭ１０３上の上記特定の領域の情報をＨＤＤ１０２に退避させる際に、所定の暗号化方式で当該特定の情報のみを暗号化して、アプリケーションの再開に必要な情報とともにＨＤＤ１０２に退避させる制御を行う。したがって、当該特定の情報の暗号化処理と、退避処理については短時間に効率よく処理できる。

また、ＣＰＵ１０１は、電源スイッチ（ＰＯＷ－ＳＷ）１０５により電源をオン状態へ遷移させる指示を受け付けた場合、ＨＤＤ１０２に暗号化して退避させた特定の領域の情報については、復号化処理を実行してＲＡＭ１０３上に復帰させる制御を行う。さらに、ＣＰＵ１０１は、暗号化していないアプリケーションに関わる情報についてはそのままＲＡＭ１０３上に復帰させる制御を行う。

したがって、当該特定の情報の復号化処理と、復帰処理については短時間に効率よく処理できる。

【００２１】

図２は、図１に示したＲＡＭ１０３の論理的構造を示す模式図である。

図２において、暗号化非対象領域２０１は、ＣＰＵ１０１を動作させるためのプログラムやハイバネーション時に暗号化の必要がないデータが含まれている。特定領域に対応する暗号化対象領域２０２は、機密情報を含み、ハイバネーション時に暗号化が必要なデータが含まれている。

【００２２】

例えば、ソフトウエアが動作する際に一時的にＲＡＭ１０３にデータを保持するが、その際は暗号化非対象領域２０１にそれを配置する。ただし、ソフトウエアがパスワード等のセキュリティに関連するデータを扱う処理の場合は、データを暗号化対象領域２０２に配置する。以下、本実施形態における情報処理装置の電力制御について説明する。

【００２３】

図３は、本実施形態を示す情報処理装置の電力制御方法を説明するフローチャートである。本例は、ハイバネーション状態に入る際に一部のデータを暗号化して退避する処理例である。なお、各ステップは、ＣＰＵ１０１がＨＤＤ１０２に記憶される制御プログラムを実行することで実現される。本実施形態では、特定にハイバネーションモードに基づく処理のうち、特に上述したアプリケーションの機能に必要な機密情報（使用権限に関わる情報を含む）の管理処理と、暗号化、復元化処理に伴う情報の退避制御、復元制御について詳述する。

【００２４】

ＣＰＵ１０１がＰＯＷ－ＳＷ１０５がＯＦＦされたことを、ＩＮＴＣ１０４を経由して検知すると、ハイバネーション状態に入る処理が開始される（Ｓ３０１）。ここでは一例

として、ＰＯＷ－ＳＷ１０５がＯＦＦされたことをきっかけとしているが、図示しない操作部からの指示や、図示しないタイマーなどからの信号がきっかけとなる場合がある。

【００２５】

続いて、各種ハードウェアの状態等を保持するために、終了処理が実行される（Ｓ３０２）。本実施形態において、終了処理は、電源断に備えてのハードウェアの終了処理や、ハイバネーションから復帰する際に再設定するための設定の保持処理などを指す。設定は主にＲＡＭ１０３に保持される。終了処理が終了すると、ＣＰＵ１０１は、ＲＡＭ１０３の内容をＨＤＤ１０２に退避する処理を開始する。具体的には、最初に、ＣＰＵ１０１は、暗号化非対象領域２０１をＨＤＤ１０２に退避する（Ｓ３０３）。

【００２６】

次に、ＣＰＵ１０１は、暗号化対象領域２０２の暗号化処理を行う（Ｓ３０４）。ここで、暗号化のアルゴリズムについては特に制約はないが、強固な暗号アルゴリズムを使用すると、それだけＲＡＭ１０３を消費する傾向にある。

また、暗号アルゴリズムが使用する鍵情報も一時的にＲＡＭ１０３に保持する必要がある。その際は、暗号処理のために追加でＲＡＭ１０３領域が必要になるが、その場合は退避済の暗号化非対象領域２０１を使用してもよい。なお、ＲＡＭ１０３の暗号化対象領域２０２のサイズや、アドレスを自動的に割り当てる構成とするが、暗号化処理の方式に応じてそのサイズ等を変更できるように構成してもよい。また、暗号化方式は、定期的に変更できるように構成してもよい。

また、暗号アルゴリズムにより、暗号化後のデータ長が変化する。データ長が大きくなる暗号アルゴリズムを使用する際にも、退避済の暗号化非対象領域２０１を使用してもよい。

そして、最後に、ＣＰＵ１０１は、暗号化済の暗号化対象領域２０２をＨＤＤ１０２に退避する（Ｓ３０５）。全てのメモリ退避が完了した時点で、ＨＤＤ１０２にメモリ退避した旨を示すハイバネーション情報を記録して（Ｓ３０６）、本処理を終了する。

【００２７】

なお、上記Ｓ３０３からＳ３０５の処理において、暗号化非対象領域２０１と暗号化対象領域２０２を分けて退避している。しかし、暗号化処理に別途ＲＡＭ１０３を消費しない暗号アルゴリズムでは、Ｓ３０４，Ｓ３０３，Ｓ３０５の順で処理してもよい。

図４は、本実施形態を示す情報処理装置の電力制御方法を説明するフローチャートである。本例は、ハイバネーション状態から復帰する際の処理例である。なお、各ステップは、ＣＰＵ１０１がＨＤＤ１０２に記憶される制御プログラムを実行することで実現される。本実施形態では、通常電力状態に移行する要因があった場合に、特定にハイバネーションモードに基づく処理のうち、特に上述したアプリケーションの機能に必要な機密情報の管理処理と、暗号化、復元化処理に関わる処理について説明する。

【００２８】

まず、システムは電源投入されると、ＣＰＵ１０１は、Ｓ３０６で記録されたハイバネーション情報がＨＤＤ１０２に存在するかどうか判断する（Ｓ４０１）。ＨＤＤ１０２にハイバネーション情報が存在しないとＣＰＵ１０１が判断した場合は（Ｓ４０１：Ｎ）、ＣＰＵ１０１は、通常の起動処理を行い（Ｓ４０６）、本処理を終了して、通常のデータ処理に移行する。

ここで、通常の起動処理とは、ＨＤＤ１０２に保存されたオペレーティングシステムの読み込みおよび初期化処理、デバイスドライバの読み込みおよび初期化処理、他のソフトウエアの読み込みおよび初期化処理などを指す。

一方、Ｓ４０１で、ハイバネーション情報が存在した場合（Ｓ４０１：Ｙ）は、ＨＤＤ１０２に退避されたＲＡＭ１０３の情報を復元する処理を開始する。

まず、暗号化対象領域２０２に記憶されていたデータをＨＤＤ１０２からＲＡＭ１０３へ復元する（４０２）。

【００２９】

次に、暗号化対象領域２０２の復号化処理を行う（Ｓ４０３）。Ｓ３０２の暗号化処理と

同様、アルゴリズムによって処理に別途ＲＡＭ１０３が必要だったり、データ長が変化したりする場合は、暗号化非対象領域２０１を使用してもよい。
そして、最後に暗号化非対象領域２０１に記憶されていたデータをＨＤＤ１０２からＲＡＭ１０３へ復元する（Ｓ４０４）。
この時点で、ＨＤＤ１０２に退避していた全てのＲＡＭ１０３の情報が復元されたことになる。
その後、リジューム処理を行う（Ｓ４０５）。リジューム処理は、ハードウェア毎に初期設定を行ったり、終了処理３０２で保持された設定を再度ハードウェアに設定したりする処理を行う。

〔第２実施形態〕

【００３０】

次に、ハイバネーション状態に入る際に一部のデータを着脱不可能な不揮発性記憶装置に退避する実施形態について、図５，図６を使用して説明する。

【００３１】

本実施形態では、着脱不可能な不揮発性記憶装置として、図１に示したＳＲＡＭ１０６を想定している。半導体メモリで構成されるＳＲＡＭ１０６は、通常、ＣＰＵ１０１、ＲＡＭ１０３、ＩＮＴＣ１０４、ＰＯＷ－ＳＷ１０５、と共に同一の基板上に実装される。よって、着脱不可能なものとなる。なお、着脱不可能な不揮発性記憶装置であれば、必ずしもＳＲＡＭである必然性はない。

【００３２】

図５は、本実施形態を示す情報処理装置の電力制御方法を説明するフローチャートである。本例は、ハイバネーション状態に入る際に一部のデータを暗号化して退避する処理例である。なお、各ステップは、ＣＰＵ１０１がＨＤＤ１０２に記憶される制御プログラムを実行することで実現される。なお、図３に示したＳ３０１，３０２，３０６の処理に関しては、図３のフロー図の処理と同一なので割愛する。

終了処理が終了すると、ＣＰＵ１０１は、ＲＡＭ１０３の内容をＨＤＤ１０２に退避する処理を開始する。次に、ＣＰＵ１０１は、上記特定領域以外に対応する暗号化非対象領域２０１をＨＤＤ１０２に退避する（Ｓ３１３）。そして、最後に、ＣＰＵ１０１は、暗号化対象領域２０２をＳＲＡＭ１０６に退避して（Ｓ３１５）、本処理を終了する。

図６は、本実施形態を示す情報処理装置の電力制御方法を説明するフローチャートである。本例は、ハイバネーション状態から復帰する際の処理例である。なお、各ステップは、ＣＰＵ１０１がＨＤＤ１０２に記憶される制御プログラムを実行することで実現される。なお、図６に示したＳ４０１，Ｓ４０５，Ｓ４０６の処理に関しては、図４のフロー図の処理と同一なので割愛する。本実施形態では、特にハイバネーションモードに基づく処理のうち、特に上述したアプリケーションの機能に必要な機密情報の管理処理と、暗号化、復元化処理に関わる処理について説明する。

Ｓ４０１で、ハイバネーション情報が存在するとＣＰＵ１０１が判断した場合（Ｓ４０１：Ｙ）は、ＣＰＵ１０１は、ＨＤＤ１０２に退避されたＲＡＭ１０３の情報を復元する処理を開始する。具体的には、ＣＰＵ１０１は、暗号化対象領域２０２に記憶されていたデータをＳＲＡＭ１０６からＲＡＭ１０３へ復元する（Ｓ４１２）。そして、最後に、ＣＰＵ１０１は、暗号化非対象領域２０１をＨＤＤ１０２からＲＡＭ１０３へ復元して（Ｓ４１４）、本処理を終了する。

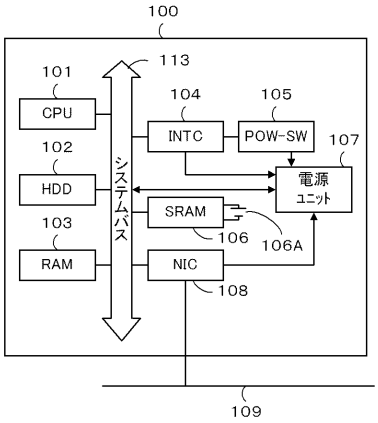
なお、上記実施形態では、ＰＯＷ－ＳＷ１０５がＯＦＦ指示を受け付けた場合に上述したハイバネーション処理を実行する例について説明した。しかしながら、図１に示すようにネットワーク対応の情報処理装置の場合、ジョブ等の受信状態を監視してハイバネーション処理を実現する構成にも本発明を適用可能である。

【００３３】

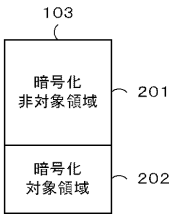
本発明の各工程は、ネットワーク又は各種記憶媒体を介して取得したソフトウエア（プログラム）をパソコン（コンピュータ）等の処理装置（ＣＰＵ、プロセッサ）にて実行することでも実現できる。

【００３４】
本発明は上記実施形態に限定されるものではなく、本発明の趣旨に基づき種々の変形（各実施形態の有機的な組合せを含む）が可能であり、それらを本発明の範囲から除外するものではない。
【符号の説明】
【００３５】
１０１　ＣＰＵ
１０２　ＨＤＤ
１０３　ＲＡＭ
１０７　電源ユニット

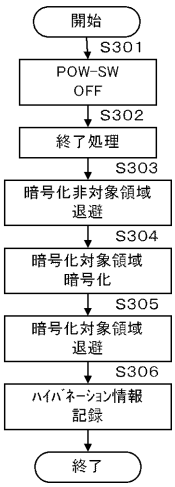
【図１】



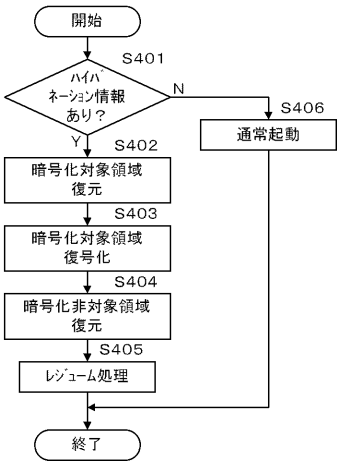
【図２】



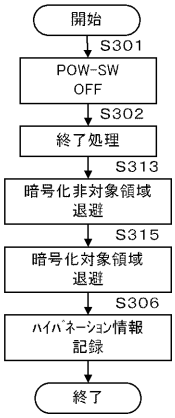
【図３】



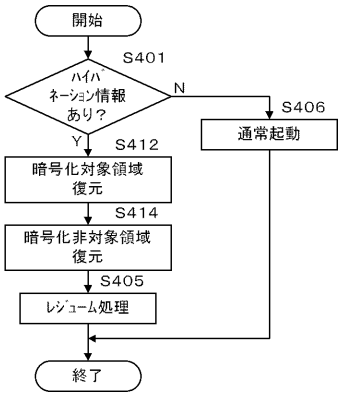
【図４】


開始
S401
ﾊｲﾊﾞﾈｰｼｮﾝ情報あり？
N
S406
通常起動
Y
S402
暗号化対象領域復元
S403
暗号化対象領域復号化
S404
暗号化非対象領域復元
S405
ﾚｼﾞｭｰﾑ処理
終了

【図５】


開始
S301
POW-SW OFF
S302
終了処理
S313
暗号化非対象領域退避
S315
暗号化対象領域退避
S306
ﾊｲﾊﾞﾈｰｼｮﾝ情報記録
終了

【図６】


開始
S401
ﾊｲﾊﾞﾈｰｼｮﾝ情報あり？
N
S406
通常起動
Y
S412
暗号化対象領域復元
S414
暗号化非対象領域復元
S405
ﾚｼﾞｭｰﾑ処理
終了

フロントページの続き

(56)参考文献 特開２００１－２０２１６７（ＪＰ，Ａ）
特開２０１０－２１４９０４（ＪＰ，Ａ）
特開２００６－２５２０２１（ＪＰ，Ａ）
米国特許出願公開第２００５／００４４４３３（ＵＳ，Ａ１）
特開平１０－２６０９１２（ＪＰ，Ａ）
米国特許出願公開第２００７／０１０１１５８（ＵＳ，Ａ１）

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｇ０６Ｆ　　１／３０
Ｇ０６Ｆ　　１／３２
Ｇ０６Ｆ　１１／１４